

**SEALED**

**AFFIDAVIT**

I, Genevieve D. Baushke, being duly sworn, do hereby depose and state the following:

**INTRODUCTION**

1. I am a Special Agent employed by the United States Department of Justice, the Federal Bureau of Investigation (hereinafter "FBI"), and as such I am a "federal law enforcement officer" within the meaning of Fed. R. Crim. P. 41(a)(2)(C) and I have been employed as a Special Agent of the FBI since 2020. I am currently assigned to the FBI Charleston Resident Agency, Charleston, West Virginia. I am a graduate of the FBI Training Academy in Quantico, Virginia, where I received special training in controlled substance investigations, white-collar crime, cyber-crime, interviewing, interrogation, evidence collection, intelligence analysis, and legal matters, among other topics. Prior to joining the FBI, I was employed with the State of Michigan as a Foster Care Specialist and an investigator for Children Protective Services

2. As a Special Agent, I have investigated federal criminal violations related to drug investigations, white collar, child exploitation, and child pornography. I have gained experience through training, as well as everyday work relating to investigations involving the receipt, possession, access with intent to view, production, importation, advertising, and distribution of child pornography that occur in the Southern District of West Virginia. I have received training in the areas of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have been the case agent or assisted others in numerous investigations involving the sexual exploitation of children. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252A(a)(2) (receipt or distribution of child pornography), 2252A(a)(5)(B) (possession of child

pornography), and 2422(b) (enticement of minors), and I am authorized by law to request a search warrant.

3. I make this Affidavit in support of an application for a search warrant for a property and residence located at 291 Oak Drive, Fayetteville, Fayette County, West Virginia 25840 ("SUBJECT PREMISES"), which is occupied by William Lawrence BRYANT, as well as the person of William Lawrence BRYANT ("BRYANT") located at the SUBJECT PREMISES. The SUBJECT PREMISES is within the Southern District of West Virginia. A written description of the SUBJECT PREMISES is set forth in Attachment A and incorporated herein. I am investigating BRYANT for violations of Title 18, United States Code, Section 2422(b), that is, the use of a means and facility of interstate commerce to attempt to persuade, induce, entice, or coerce a minor to engage in prostitution or in any sexual activity for which a person could be charged with a criminal offense; Title 18, United States Code, Sections 2252A(a)(1) and (2), that is, the transportation, receipt, and/or distribution of child pornography; and Title 18, United States Code, Sections 2252A(a)(5)(B), that is, the possession of child pornography. At the SUBJECT PREMISES, I seek to seize and search evidence and instrumentalities of criminal violations set forth above for items specified in Attachment B, incorporated herein by reference, which may be found, and to seize and search all items listed in Attachment B as instrumentalities and evidence of a crime.

4. This Affidavit is also submitted in support of an application for a search warrant for the person described in Attachment A of this Affidavit, WILLIAM LAWRENCE BRYANT. As set forth herein, there is probable cause to search the person of BRYANT, as described in Attachment A, for the items described in Attachment B, including cell phones and digital storage devices, such as USB or thumb drives, that can be concealed on the person should BRYANT be

present in the SUBJECT PREMISES. I believe probable cause exists for the issuance of a warrant to search BRYANT, as described in Attachment A, for (1) property that constitutes evidence of a federal criminal offense; (2) contraband, the fruits of a federal crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means for committing a federal criminal offense, namely 18 U.S.C. § 2252A, the distribution, transmission, receipt, and/or possession of child pornography.

5. Based on my training and experience and in related investigations and search warrants and the experience of other law enforcement investigators I have communicated with, I am aware that it is common for items of digital media, including, but not limited to laptop computers, cell phones, flash drives, cameras, and digital music devices, to be transported or stored in motor vehicles. Therefore, I request the search warrant authorize the search of any vehicles located at or near the subject premises that fall under the dominion or control of the person or persons associated with the subject premises.

6. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts necessary to establish probable cause that evidence and instrumentalities of a violations of Title 18, United States Code, Section 2422(b), and of Title 18, United States Code, Sections 2252A(a)(1), 2252A(a)(2), and 2252A(a)(5)(B) are presently located at the subject premises.

### **JURISDICTION**

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is “a district of the

United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

#### **STATUTORY AUTHORITY**

8. The investigation concerns violations of Title 18, United States Code, Sections 2252A(a)(1), 2252A(a)(2), 2252A(a)(5)(B), and 2422(b) relating to matters involving the sexual exploitation of minors.

- a) 18 U.S.C. § 2252A(a)(1) prohibits any person from knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.
- b) 18 U.S.C. § 2252A(a)(2) prohibits any person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.
- c) 18 U.S.C. § 2252A(a)(5)(B) prohibits any person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.
- d) 18 U.S.C. § 2422(b) prohibits any person, by means of the mail or any facility or means of interstate or foreign commerce or within the special maritime and territorial jurisdiction of the United States, from knowingly persuading, inducing, enticing, or coercing any individual who has not attained the age of 18 years to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense.

#### **DEFINITIONS**

9. The following definitions apply to this Affidavit and its Attachments.
- a) The term “**minor**,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
  - b) The term “**child erotica**” means materials or items that are sexually arousing to persons having a sexual interest but that are not necessarily

in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

- c) The term “**child pornography**,” as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable form, that of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
- d) The term “**sexually explicit conduct**,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.
- e) The term “**visual depiction**,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disk or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.
- f) The term “**computer**,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
- g) The terms “**records**,” “**documents**,” and “**materials**,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph

records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact disks, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

- h) **“Internet Service Providers”** (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-locations of computers and other communications equipment.
- i) **“Internet Protocol address”** (“IP address”), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static if an ISP assigns a user’s computer a particular IP address each time the computer accesses the Internet.
- j) **“Websites”** consist of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (“HTML”) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (“HTTP”).
- k) **“Chat,”** as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.
- l) **“Cloud-based storage service,”** as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and

tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

- m) **“Computer hardware,”** as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data- processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).
- n) **“Computer software,”** as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- o) **“Computer passwords and data security devices,”** as used herein, consist of information designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- p) **“Mobile applications,”** as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.
- q) **“Peer to Peer File Sharing” (“P2P”)** is a free open source software process that allows computer users, utilizing the same file sharing software, to connect to each other and directly access files from one another’s computer hard drive. The files to be shared with others across the Internet are selected as shareable by each individual computer user. This action is usually done by the

computer user who will place files he/she wishes to share into a specific folder often times titled "Shared Folder". The software only allows remote users to access this "shared folder" and thus prevents access to the rest of the computer hard drives contents. Some examples of peer to peer files sharing software are Napster, Kazaa, Grokster, Gnutella, eMule, Morpheus, Phex, Ares, BitTorrent, etc.

- r) "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

**BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS,  
THE INTERNET, AND EMAIL**

10. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

11. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). Darkroom facilities and a significant amount of skill were required in order to develop and reproduce the photographic images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their detection by the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

12. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication,

distribution, and storage.

13. Child pornographers can now transfer photographs from a camera in a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through FTPs to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials among pornographers.

14. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers and other electronic devices such as cell phones or even gaming consoles has increased tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

15. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

16. Collectors and distributors of child pornography also use online resources

to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Inc., and Google, Inc., among others. The online services allow a user to set up an account with remote storage. Even in cases where online storage is used, however, evidence of child pornography can often be found on the user's computer.

**SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER  
AND ELECTRONIC DEVICE SYSTEMS**

17. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers and other electronic devices, I know that data can be stored on a variety of computer systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage.

18. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such

information is often maintained on the computer indefinitely until overwritten by other data.

19. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- a) Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;
- b) Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;
- c) The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and
- d) Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

20. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

- a) The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and
- b) In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit ("CPU"). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

21. As described further in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B), of any device belonging to or used by BRYANT, or where ownership cannot be determined.

22. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

- a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b) Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- d) Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- e) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

23. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

- a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b) Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c) The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatory or exculpatory the computer owner.
- d) Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of

computer or electronic storage media access, use, and events relating to the crime under investigation.

- e) Some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user.
- f) Moreover, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).
- g) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- h) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- i) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- j) I know that when an individual uses a computer to distribute or attempt to distribute child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The

computer is also likely to be a storage medium for evidence of a crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

24. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

25. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

26. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and its attachments and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

**BIOMETRIC ACCESS TO DEVICES**

27. This warrant permits law enforcement to compel BRYANT to unlock any devices requiring biometric access subject to seizure pursuant to this warrant. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

28. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

29. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.

Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

30. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

31. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

32. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

33. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

34. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of BRYANT to the fingerprint scanner of the devices found at the SUBJECT PREMISES; (2) hold the devices found at the SUBJECT PREMISES in front of the face of BRYANT and activate the facial recognition feature; and/or (3) hold the devices found at the SUBJECT PREMISES in front of the face of BRYANT and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that BRYANT state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement

to compel BRYANT to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

**CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS**

35. Based upon my knowledge, experience, and training in criminal investigations, particularly those that focus on child exploitation, as well as the training and experience of other law enforcement officers trained in child exploitation and child pornography investigations with whom I have had discussions, there are certain characteristics common to individuals involved in the possession, receipt and distribution of child pornography:

- a) Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b) Collectors of child pornography may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce or to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c) Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d) Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.
- e) Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of

time even after the individual “deleted” it.<sup>1</sup>

- f) Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they collect their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- g) Collectors of child pornography prefer not to be without their child pornography for any prolonged time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. It has long been recognized by professionals dealing with persons involved with child pornography that child pornography has enduring value to those involved in the sexual exploitation of children. Such persons rarely, if ever, dispose of their sexually explicit material. Those materials are often treated as prized possessions. Individuals involved in child pornography almost always maintain their materials in a place that they consider secure and where the materials are readily accessible. Most frequently, these materials are kept within the privacy and security of their own homes. These materials are often kept on their person in forms of media storage devices such as thumb drives and cellphones in their pants pockets and on their keychains.
- h) Further, it is common for such users to save and transfer the pornographic images and/or pornographic video of children from one computer to another because the images are generally difficult to obtain securely.

36. Your Affiant believes that given the continuing nature of possession of child pornography and the general character of such offenders as “collectors” and “hoarders,” there is probable cause to believe that evidence of violations of federal law, including, but not limited to, 18 U.S.C. §§ 2252A(a)(2) (receipt or distribution of child pornography), 2252A(a)(5)(B) (possession of child pornography), 2422(b) (enticement of a minor) will be present in the

---

<sup>1</sup> See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because “staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology”); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

SUBJECT PREMISES, and on the person of BRYANT, as described in Attachment A, when the search is conducted. Thus, even if the individual associated with the SUBJECT PREMISES, believed at this time to be BRYANT, uses a portable device (such as a mobile phone) to access the internet and child pornography, there is probable cause that evidence of this access will be found in the SUBJECT PREMISES in addition to being on his person.

**The Onion Router (also known TOR)**

38. TOR is a special network of computers on the internet distributed around the world, designed to conceal the true Internet Protocol (IP) addresses of computers accessing the network, and thereby, the locations and identities of the network's users. TOR also enables websites to operate on the network in a way that conceals the true IP addresses of the computer services hosting the websites, which are referred to a "hidden services" on the TOR network.

39. The TOR network can be accessed through special browser applications uploaded onto an electronic device such as the TOR browser app or Red Onion app. Use of these browser applications allow users to access the internet anonymously.

**PROBABLE CAUSE**

40. On or about June 10, 2021, while undergoing an interview with federal agents as part of a proffer agreement in Case No. 1:21-cr-00080 out of the United States District Court for the District of Delaware, subject SETH BAYLESS ("BAYLESS"), provided the following information. BAYLESS came to know BRYANT through Child Sex Abuse Material (CSAM) channels on the social media messaging service Telegram in 2017. BAYLESS related that BRYANT used several usernames across various platforms, including: "Buttons," "Butt0ns," or "Butt0nz." BRYANT would pretend to be a girl while on Telegram in a bid to attract underage male interaction. Eventually, BRYANT told BAYLESS that he was in fact a male, and they

became friends over a shared interest in nude boy model sets. BAYLESS related that BRYANT would send photos both of himself and CSAM to BAYLESS through the Telegram application. BAYLESS described BRYANT, known to him as "Billy," as a 31-year old male with a birthdate in May 1990. He described him as blonde haired with blue eyes and residing in a town in West Virginia that celebrates a local holiday: Bridge Day. BAYLESS obtained this information during conversations with BRYANT on Telegram.

40. The FBI Child Exploitation Unit (CEOU) took the information, provided by BAYLESS, and ran those identifiers through open source databases and West Virginia DMV. The open source databases included Accurint and Clear. As a result, CEOU was able to identify BRYANT as an individual who has similar characteristics to user "Billy Butt0ns." FBI Baltimore provided information that originated from Norwegian Law Enforcement and information provided during a proffer with BAYLESS to FBI Charleston. FBI Baltimore also provided BRYANT'S expired driver's license.

41. Using the information provided by FBI Baltimore, I confirmed that BRYANT's DMV photo indicates he has blue eyes. I confirmed that BRYANT's DMV record indicates BRYANT's date of birth is in May 1990, and his address of record is 291 Oak Drive, Fayetteville, WV 25840. On March 8, 2022, the Post Office reported BRYANT receives mail at 291 Oak Drive, Fayetteville, WV 25840.

42. Bridge Day is celebrated on the New River Gorge Bridge in Fayetteville, WV every third weekend in October.

43. On March 20<sup>th</sup>, 2022, Special Agent Georgia Marshall and I conducted surveillance on BRYANT. During surveillance, Special Agent Georgia Marshall and I observed BRYANT walk out of the front door and onto the porch of the residence at 291 Oak Drive, Fayetteville, WV

25840. Special Agent Georgia Marshall and I observed BRYANT walk to the garage, get on his dirt bike, and drive to his place of employment. During surveillance at his place of employment, I observed BRYANT to have blue eyes and hair that is light brown or dark blonde in color.

44. The physical description provided by BAYLESS matches that of William Lawrence BRYANT. The personal identifiers provided by BAYLESS matches those belonging to BRYANT. The location description provided by BAYLESS matches the area where BRYANT resides. I conducted a computerized search of BAYLESS's criminal justice information using the National Crime Information Center (NCIC). The NCIC is a computerized index of criminal justice information such as criminal record history information, fugitives, stolen properties, and missing persons. My NCIC search for BAYLESS revealed no prior convictions for crimes of deceit or fraud.

45. BAYLESS also related that in addition to Telegram, BRYANT shared CSAM using TOR. CSAM shared by BRYANT was uploaded to the TOR website "BoysTown," a website used primarily for storing and sharing CSAM. "BoysTown" was raided and shut down by European law enforcement authorities in May 2021.

46. BAYLESS related that BRYANT accessed BAYLESS'S computer in January 2021 to set up ways to browse and share CSAM to avoid detection. BRYANT did this using Tails. Tails is a portable operating software that can be installed on a computer, acting as a "computer within a computer" in order to browse and store CSAM while avoiding detection. BAYLESS stated that BRYANT used TeamViewer, an app capable of remotely accessing computer systems, to install Tails onto a USB thumb drive on behalf of BAYLESS.

47. BAYLESS also related that BRYANT taught him how to "bait" boys on the internet. "Baiting" is a method of producing CSAM by inducing a conversation with a victim over

a video messaging application like Omegle or Skype (two platforms that permit users to engage in live video chats) using a manipulated video that makes the victim believe he is in a conversation with a female. The victim would then be asked to produce videos of himself masturbating or to send nude images. BRYANT produced CSAM through “baiting,” which was later found during a law enforcement search of BAYLESS’s phone, to include a 20-minute video of a 15-year old male, “Shane” masturbating. BRYANT shared the CSAM he created by “baiting” online and marked his produced CSAM with a logo of a Nintendo controller with the word BUTTONS underneath.

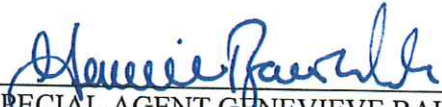
48. BAYLESS related that BRYANT first produced CSAM via baiting in 2004 and began to produce CSAM in 2007. BAYLESS stated that BRYANT has at least two computers, multiple hard drives, and several mobile phones that he keeps in the SUBJECT PREMISES for storage of CSAM. BAYLESS stated that he was aware BRYANT’s computers were encrypted with a 20-digit passcode. BRYANT has multiple mobile phones that BRYANT is unable to gain access to due to being “broken”. The extent to which these phones are broken is unknown. Additionally, BAYLESS stated that he was aware BRYANT stored most of his CSAM “collection” on a desktop computer located at the SUBJECT PREMISES.

### **CONCLUSION**

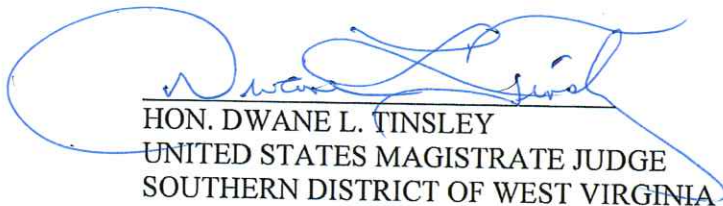
49. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

50. Moreover, I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Further your Affiant sayeth naught.

  
SPECIAL AGENT GENEVIEVE BAUSHKE  
DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this  
31 day of March, 2022.

  
HON. DWANE L. TINSLEY  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF WEST VIRGINIA